ATTACHMENT R – DPSCS ITCD TECHNOLOGY ARCHITECTURE STANDARDS (TAS)

The following pages contain 42 standards identified by a TAS reference number.

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
1	**Access Control**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	Network Services	Directory Service
Security	Identity Control	Authentication
	Security Services	Firewall Spam Control
	Security Management	Host Intrusion Protection Network Intrusion Protection

Description

Logical access control within DPSCS is provided at the network, operating system, and application level.

- **Network Access Control.** Network access controls can be provided by a variety of mechanisms both alone and in combination. However, the primary method of providing network access control in an enterprise environment is via a firewall.
- **System Access Control.** Access control can also be provided by the client or server operating system. Host access control can also be provided at the operating system level via third party products that are designed to enhance an operating system's native access control facilities.
- **Application Access Control.** Application access control can be provided by either the underlying Database Management System (DBMS) or by the application itself.
- **Content Filtering.** Access control can also be based on content or sites. The motivation to block certain content or sites is driven by DPSCS acceptable use policy.

Tactical (0-2 years)	Strategic (2-5 years)
Account/Password Synchronization IronPort (Hardware version: C350 Software: 5.0.0-231) CA Top Secret 8.0	Single Sign-On PKI (X.509) Server-based Firewalls IDS/IPS
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
Checkpoint VPN (Core: NGX 60 HFA04, Edge firmware: 7.0.25) Cisco ACL MS Active Directory Security Group Membership (Windows 2000 Forest Functional Level & Windows 2000 Native Domain Functional Level) NTFS ACLs (Windows NT 4.0, Windows 2000, & Windows 2003) CA Top Secret 5.3 SQL Authentication (2000 & 2005) Local System Authentication (Windows NT 4.0, Windows 2000, & Windows 2003) Websense 6.2 Watchguard (Hardware: X8500e-F / Software: 8.3) RSA ACE Server 5.2 Role-based Access Control DBMS TCP/IP Version 4 Citrix MetaFrame XP Presentation Server FR4	

Relevant Standards

- 802.1x, Kerberos, X.509

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
2	**Routers / Switches**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	WAN	WAN Routing WAN Transport
	LAN/MAN	LAN/MAN Routing LAN/MAN Transport
	Wireless	Wireless Routing Wireless Transport

Description
Access routers and switches connect subnets to the distribution layer. In some cases, the access router/switch functionality is combined with the distribution and workgroup layer switches so that a single box performs the functions of access, distribution and/or workgroup layers.

Core routers are part of the backbone, which also contains all the high-speed transport media. This layer does not provide any packet manipulation.

Distribution routers and switches connect the access layer to the backbone network. The distribution layer directs and filters traffic between access layer and the core layer.

Tactical (0-2 years)	Strategic (2-5 years)
Retirement (to be eliminated)	**Containment (no new development)**
Cisco 7513, 3810, 4006, 2500	
Baseline (today)	**Emerging (to be tracked)**
Access: Cisco 2800, 3810, 2500, 2600, 3600, 3700, 7200, 3550, 3845 Core: Cisco 6513, 7513, 4006, 7200, 7400, 3750, 3845 Distribution: Cisco	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
3	**Application Server**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Operating System	Server OS Mainframe OS

Description
An *application server* is a modern form of platform middleware. It is system software that resides between the operating system on one side, and the external resources - such as DBMS, communications and Internet services - on another side, and the users' applications on a third side.
At runtime, the application server is to act as host (or container) for the user's business logic while facilitating access and performance of the business application. The application server must perform despite the variable and competing traffic of client requests, hardware and software failures, the distributed nature of the larger-scale applications, and potential heterogeneity of the data and processing resources required to fulfill the business requirements of the applications.
The following classifications apply to standalone applications servers, not application servers that are included with a multi-tier COTS product.

Tactical **(0-2 years)**	**Strategic** **(2-5 years)**
WebSphere 7.x Microsoft .NET Server 2.0 Oracle 9i Application Server Citrix MetaFrame XP Presentation Server FR4 IBM Rational Application Dev (J2EE) 7.x ASP/ASP.Net 2.0 VB.Net 2.0 HTML/CSS-HTMS 4 CSS 2 IBM zOS 1.7	
Retirement **(to be eliminated)**	**Containment** **(no new development)**
Fox Pro Oracle 8	Windows NT 4.0 Server Windows 2000 MS Visual Basic 6.3 VBA 9.0.4402 MS Access 9.0.4402 Centura/Gupta Team Developer 3.0
Baseline **(today)**	**Emerging** **(to be tracked)**
Windows 2003 IBM AIX 5.2 IBM zOS 1.4 Linux (Gentoo & RedHat Distributions) WebSphere 6.0.2.5 Microsoft .NET Server 2.0 Oracle 9i Application Server IBM Rational Application Dev (J2EE) 6.0.x ASP/ASP.Net 2.0 VB.Net 2.0 HTML/CSS-HTML 4 CSS 2 Centura/Gupta Team Developer 3.0	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
4	**Availability**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Enterprise Management	Fault	System Monitoring

Description

Availability - Application Management is the monitoring, collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for application servers and application services. This discipline involves using automated tools to avoid problems (e.g., automatically increasing file space when it reaches a threshold) and job scheduling to reduce operator error and improve the availability of batch applications and data.

Availability - Database Management is collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for database management systems.

Availability - Server Management is collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for servers and end-to-end connections.

Availability - Storage Management is collecting and correlating performance, event and availability statistics to predict and, thus, avoid potential downtime for storage subsystems. Tactical deployments of vendors for SAN management, storage resource management, provisioning, hierarchical storage management and storage policy management have been identified below.

Availability Management - Network management includes the administrative services performed in managing The DPSCS Network, including network devices, network topology and software configuration, monitoring network performance, maintaining network operations, and diagnosing and troubleshooting problems. Network management requires the skillful integration of software tools, management processes and resources to provide enterprise managers with a coherent view of network availability and performance. This task becomes increasingly difficult as business applications become more reliant on and intertwined with network infrastructure and as users come to expect nearly unlimited, “free” bandwidth. A Manager of Managers network management capability must be developed based on Simple Network Management Protocol (SNMP) version 3, and all network management solutions must interface to HP OpenView for compliance to this architecture.

Tactical (0-2 years)	**Strategic (2-5 years)**
HP Openview NNM 7.5	Event Correlation and Alerting (Microsoft Office Manager/NetIQ App Manager)
Retirement (to be eliminated)	**Containment (no new development)**
	BMC Patrol Big Brother
Baseline (today)	**Emerging (to be tracked)**
Cisco Works SMS 2003 Quest Spotlight for Exchange Version 4 TMON for MVS 3.1 TMON for CICS 2.2 TMON for DB2 3.3 TMON for IMS 2.0 TMON for MQ Series 2.0	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
5	**MAN /WAN Optical Networking**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	WAN	WAN Routing WAN Transport

Description
This TAS addresses optical networking when implemented as part of the network backbone. Storage-Area Networks (SANs) can also use this technology, but those standards will be architected in the server environment area of the Enterprise Architecture. These technologies are also used to attach to the backbone.

Tactical (0-2 years)	Strategic (2-5 years)
Retirement (to be eliminated)	**Containment (no new development)**
	McData (SPHEREON 4500)
Baseline (today)	**Emerging (to be tracked)**
Cisco 9216 Cisco 9509 Emulex, QLogic HBA	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
6	**MAN / WAN Transport**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	WAN	WAN Routing WAN Transport
	LAN/MAN	LAN/MAN Routing LAN/MAN Transport

Description
On a limited basis, Packet over SONET (Synchronous Optical Network)-based transport technology is used in the MAN/WAN environment as provided by service providers. Packet-over-SONET/SDH (POS) enables core routers to send native IP packets directly over SONET/SDH frames.

DPSCS is considering the future use of multi-protocol label switching (MPLS) as a transport mechanism. MPLS is a generic networking technique that combines many of the desirable features of technologies such as ATM and frame relay with the features of IP. MPLS can deliver alternative QoS services for potential voice-over-IP deployment in the future.

Tactical (0-2 years)	Strategic (2-5 years)
SONET	
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
SONET Frame Relay Microwave ATM	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
7	**Communication Middleware**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Integration	Data Integration	Data Exchange

Description
Communication middleware helps programs talk to other programs. It is software that supports a protocol for transmitting messages or data between two points as well as a system-programming interface to invoke the communication service. Message-Oriented Middleware also provides for the safe and reliable delivery of messages.

Today's communication middleware generally runs on Internet-based protocols, but also may implement higher-level protocols, including industry standards and proprietary protocols, and it may run over the Internet or private networks.

Although simple forms of communication middleware do not inherently provide them, a variety of services are provided by more sophisticated products. Such features include reliable delivery, transactional support/integrity, message queuing, offline message handling, once-and-only-once delivery as well as first-in, first-out and other message-ordering variations.

Although communication middleware is an essential requirement for application integration projects, no single solution or industry standard can address requirements for every integration problem or scenario.

Tactical (0-2 years)	**Strategic (2-5 years)**
Windows Communication Foundation (WCF) Java Messaging Service (JMS) Microsoft Message Queue (MSMQ) WebSphere MQ 6.0	
Retirement (to be eliminated)	**Containment (no new development)**
	COM/ Distributed COM Post Office Protocal (POP)/Simple Mail Transfer Protocol (SMTP)
Baseline (today)	**Emerging (to be tracked)**
COM/Distributed COM MSMQ POP/SMTP Java Message Service (JMS) IBM WebSphere MQ (IBM MQSeries) 5.3	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
8	**Communication Protocol**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	WAN	WAN Routing WAN Transport
	LAN/MAN	LAN/MAN Routing LAN/MAN Transport
	Wireless	Wireless Routing Wireless Transport

Description
Communications protocols define the rules for sending blocks of data from one node in the network to another node and are normally defined in layers. A protocol specification defines the operation of the protocol and may also suggest how the protocol should be implemented.

Minimizing the number of protocols in use can benefit DPSCS by simplifying the environment and improving interoperability. Use of TCP/IP as the primary protocol on the DPSCS Network and subnets is recommended. SNA will be converted to IP. Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. DLSw can be used to reduce SNA traffic over the WAN. Video will use the H.32x standard. SNA will be contained with no more implementations. Minimizing the number of network protocols will have a significant return on the total cost of ownership (TCO) for network management.

Tactical (0-2 years)	Strategic (2-5 years)
TCP/IP	TCP/IP
Retirement (to be eliminated)	**Containment (no new development)**
SNA DLSw	NetBIOS/NetBEUI SNA
Baseline (today)	**Emerging (to be tracked)**
TCP/IP Version 4 SNA	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
9	**Confidentiality**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Security	Security Services	Encryption

Description
The primary method of protecting confidentiality of information is via encryption. In addition to sensitive business data, there is also data about the network and systems themselves that need to be encrypted in order to prevent attacks.

Tactical (0-2 years)	**Strategic (2-5 years)**
SSL PPI	
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
SSL SSH AES Blackberry Transport Encryption Hardware Tokens (algorithms)	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
10	**Configuration Management Software**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Enterprise Management	Operations Management	Configuration Management

Description
Configuration Management is the documentation and management of the technical elements and relationships in the IT infrastructure, application and business process components. This discipline is an underpinning of problem, change and availability management. Configuration Management provides an understanding of how applications, business processes and IT elements relate, so that the impact or resolution priority of a change or problem (e.g., outage) can be determined. Which component relationships are tracked and how the information is used depend on the task required:

- Client configuration management tools focus on configuring and deploying operating system, patches and applications to client devices.
- Server configuration management tools focus on configuring and deploying operating system, patches, applications and content to servers.
- Network configuration management tools focus on documenting configuration files, auditing changes and deploying updates to network devices.
- IT service configuration management tools focus on discovering and documenting the relationships among the components that comprise an IT service — from end-user devices to servers, networks, storage, applications and data. These tools are prerequisites for achieving success with service-level, change, problem, availability, and performance management.

Tactical (0-2 years)	**Strategic (2-5 years)**
HP Openview NNM 7.5 Remedy Version 6 Active Directory Group Policy (Windows 2003 Forest Functional Level & Windows 2003 Native Domain Functional Level)	
Retirement (to be eliminated)	**Containment (no new development)**
WSUS Version 2 – 6 months	Big Brother BMC Patrol
Baseline (today)	**Emerging (to be tracked)**
SMS 2003 WSUS Version 2 Dell OpenManage 3.70 Visio 2003 Cisco Works ScriptLogic Desktop Authority 7.5 Active Directory Group Policy (Windows 2000 Forest Functional Level & Windows 2000 Native Domain Functional Level) MTAF Web Site	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
11	**Data Management Middleware**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Integration	Data Integration	Database Connectivity

Description
Data management middleware functionality helps programs, including application programs and database management systems (DBMS), read from and write to remote databases or files.

The most widespread forms of middleware today are the remote database access and remote file access middleware bundled into a DBMS or a network operating system, respectively. These support traditional two-tier client/server architectures and can also be used for more sophisticated multi-tier applications. All modern relational DBMSs include a networking capability so that the DBMS engine can optionally be called from a client application located elsewhere.

Tactical (0-2 years)	Strategic (2-5 years)
IBM DB2 Connect JEE 1.4 Object Linking and Embedding Database (OLE DB) 2005.90.2047.00 OLEDB Oracle Net Services 10.00.00.00	
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
JEE 1.4 Object Linking and Embedding Database (OLE DB) 2005.90.2047.00 Open Database Connectivity (ODBC) 9.02.00.02 IBM DB2 Connect	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
12	**Data Warehouse Database Server**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Database Management	Data Warehouse

Description
Data Warehouse (DW) database functional requirements are different than OLTP DBMS in that they support large databases, complex multi-table join processing and schema support, and have specialized index technology, workload management, and data partitioning capabilities. Most importantly, they support parallel capabilities (e.g., I/O, query and operations), and parallel utilities (e.g., backup/recovery and reorganization). DW databases are generally not updated real time, but are frequently updated via over night, batch oriented processes.

Tactical (0-2 years)	Strategic (2-5 years)
IBM DB2 7.1 IBM IMS 8.1	DB2 8.1
Retirement (to be eliminated)	**Containment (no new development)**
	Microsoft Access 9.0.4402 Centura/Gupta SQLBase 8.5
Baseline (today)	**Emerging (to be tracked)**
IBM DB2 6.1 Microsoft SQL Server Oracle 9.2.06 / 10.1 IBM IMS 6.1 IBM VSAM Mircosoft Access	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
13	**Email Server OSs**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Delivery Server	Messaging Server

Description

Email server operating systems (OSs) allocate system resources for the computers (servers) that run DPSCS's enterprise electronic mail applications. Messaging client software includes applications that run on workstations and enable peer-to-peer, asynchronous communications Messaging protocols are the formal specifications that define data exchange procedures. Messaging servers are enterprise applications that run on a central computer and enable synchronous and asynchronous, peer-to-peer communications.

Resource Scheduling is a utility or feature that facilitates commitment of any resource(s) (person, room, office, subjects, equipment, etc.) for either a single time period or a series of times. These products may provide interfaces to project management, email calendaring, workflow, inventory management and other applications. DPSCS currently uses Microsoft Exchange Scheduling to meet most general-purpose scheduling needs. This TAS addresses the more complex business requirements that necessitate invoking business logic or an interface to other functions to manage the scheduling of a resource.

Secure email is a method of establishing trust and securing email communications and attachments exchanged between DPSCS and external users.
The technology elements documented in the Secure Email TAS provide for the following:

- An alternative method of secure email communication where a PKI-based S/MIME solution is not practical (i.e., imposes an undue technical complexity or cost burden on an external partner)
- The capability to establish trust between internal and external senders and recipients
- The capability for a DPSCS user to send a secure email communication and/or attachment that is received and read by a recipient who is inside or outside the DPSCS infrastructure
- The capability for an external user to send a secure email communication and/or attachment that is received and read by a recipient who resides inside the DPSCS infrastructure
- The minimization of operational impact and cost on DPSCS and external users

Tactical (0-2 years)	Strategic (2-5 years)
	The use of PKI/Digital Certificates to secure Exchange MS Exchange 2007
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
MS Exchange 2003 Certified Mail Blackberry	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
14	**Enterprise and Mid-Range Server Operating System**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Operating System	Server OS

Description

Enterprise servers consist of the platform hardware and the operating system that together support the operating environment to support application and database servers that serve the entire DPSCS organization. They typically serve hundreds, if not thousands, of concurrent users and utilize high availability and redundant configurations to minimize downtime.

Mid-range servers consist of the platform hardware and operating system that together support the operating environment for applications and databases that serve a smaller group of users. Because the distinctions between enterprise and mid-range servers depend on subjective estimates of workload magnitude, this TAS addresses both enterprise and mid-range servers. These standards are meant to provide guidance when selecting a server for a new application or when upgrading the server environment for an existing application. It cannot replace the capacity planning and operational support analysis needed to ensure the new server environment (including storage subsystems and peripherals) that is not addressed here is capable of meeting the size, maintainability, performance, and availability requirements of the business. This TAS specifically provides baseline information and the future direction for deploying enterprise and mid-range servers at DPSCS in terms of the preferred operating systems.

Tactical (0-2 years)	Strategic (2-5 years)
IBM AIX IBM z/OS 1.7 Microsoft Windows Server 2003 Sun Microsystems SUSS	
Retirement (to be eliminated)	**Containment (no new development)**
Microsoft Windows NT Server – 18 months Sun Microsystems – 6 months	Windows NT 4.0 Server Windows 2000 Server UNIX from other vendors
Baseline (today)	**Emerging (to be tracked)**
Windows 2003 Server IBM AIX 5.2 IBM zOS 1.4 Linux (Gentoo and Red Hat distributions) Microsoft Windows 2000 Microsoft Windows NT Server Sun Microsystems UNIX	Windows “Longhorn” Server

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
15	**Enterprise and Mid-Range Server Platform Processor**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Hardware Platform	Server

Description

Enterprise servers consist of the platform hardware and the operating system that together support the operating environment to support application and database servers that serve the entire DPSCS organization. They typically serve hundreds, if not thousands, of concurrent users and utilize high availability and redundant configurations to minimize downtime.

Mid-range servers consist of the platform hardware and operating system that together support the operating environment for applications and databases that serve a smaller group of users. Because the distinctions between enterprise and mid-range servers depend on subjective estimates of workload magnitude, this TAS addresses both enterprise and mid-range servers. These standards are meant to provide guidance when selecting a server for a new application or when upgrading the server environment for an existing application. It cannot replace the capacity planning and operational support analysis needed to ensure the new server environment (including storage subsystems and peripherals) that is not addressed here is capable of meeting the size, maintainability, performance, and availability requirements of the business. This TAS provides baseline information and the future direction for deploying enterprise and mid-range servers at DPSCS in terms of the preferred hardware platform.

Tactical (0-2 years)	Strategic (2-5 years)
Virtualization	
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
IBM P-Series IBM Blade Server Series Dell Poweredge Intel Pentium	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
16	**Enterprise Directories**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	Network Services	Directory Service

Description
Enterprise directories list and/or describe users and services on the DPSCS network and are typically used in conjunction with the enterprise messaging systems.

Tactical (0-2 years)	Strategic (2-5 years)
Active Directory (Windows 2003 Forest Functional Level & Windows 2003 Native Domain Functional Level)	LDAP Directory synchronization/integration
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
Active Directory (Windows 2000 Forest Functional Level & Windows 2000 Native Domain Functional Level)	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
17	**Enterprise Reporting Tool Standards**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Enterprise Management	Operations Management	Configuration Management

Description
An enterprise reporting tool is one that allows DPSCS to gain a better understanding of its operations by putting critical information in the hands of all those who need it – employees, managers, partners, and the public.

An enterprise reporting tool must be configurable to meet the needs of its user base, capable of accessing information assets in the enterprise based on access rights, and must support wide-scale deployment.

Enterprise reporting tools as defined above generally contain several types of functionality, from generic reporting capabilities (including report design) to robust ad hoc querying and online analytical processing (OLAP) capabilities or business intelligence (BI).

Tactical (0-2 years)	Strategic (2-5 years)
Adobe Acrobat 8 MS Office 2007 SAS 9.1.3 SPSS 4.1	
Retirement (to be eliminated)	**Containment (no new development)**
	MS Office 2000 SAS
Baseline (today)	**Emerging (to be tracked)**
Adobe Acrobat 6.0, 7.0 Visio 2003 MS Office 2000, 2002, 2003 Oracle 9i App Server SAS 8.2 SPSS 4.1	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
18	**Event Management, Monitoring and Analysis**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Enterprise Management	Fault	System Monitoring Network Monitoring Power Monitor/Management

Description
Enterprise *event management* systems support the acceptance of events from elements in the IT infrastructure; consolidate, filter and correlate those events; notify the appropriate IT operations personnel of critical events; and automate corrective action where possible.

Event management helps IT operations personnel contend with the deluge of events that come in from the IT infrastructure by narrowing the events to the likely cause of the problem and associating them with the potential business impact. The goals are to improve the mean time to isolate and repair problems and to prioritize problem resolution support efforts according to business process value.

Event Management - Managers of Managers, or “MoM” products generally run on Unix or Windows and provide functionality in the following three key areas:

1. Event Collection/Consolidation: the ability to accept events from one or more of the following types of IT elements:
- System (hardware and operating system)
- Network
- Storage
- Database
- Application (packaged off-the-shelf and/or custom applications).

2. Event Processing/Correlation: the automated, out-of-the-box ability to process/correlate events through one or more of the following techniques:
- De-duplication/filtering (For example, when multiple, repetitive events are received for the same problem on the same element, store the event once and increase a counter indicating the number of times it has been received, rather than flooding the user's screen with redundant events.)
- Event suppression (For example, suppress the sympathetic events that occur when elements downstream from a known problem are unreachable.)
- State-based correlation at the object level (For example, if a "link down" event is received for a router interface that then corrects itself and generates a subsequent "link up" event, the event management system correlates the two and clears the original link down event.).

3. Event Presentation: the ability to present event data to the IT operations staff in one or more of the following ways:
- On the console screen using color and sound (visual and audible alarms)
- Through a Web interface
- By pager and e-mail
- By logical groupings (presenting groups of events that relate to business processes, IT services, departments, geographic regions or any other arbitrary, user-defined grouping).

Event Monitoring and Analysis –

Vulnerability Analysis. Internet-based attack tools are becoming increasingly sophisticated and increasingly easy to use. DPSCS's network could contain vulnerabilities that attackers can exploit to gain access, even when DPSCS has secured the network perimeter with firewalls and intrusion detection systems. In order to proactively find and plug such holes DPSCS will require the use of both vulnerability assessment products and vulnerability assessment services.

System Monitoring and Logging. Identifying and reacting to security incidents in real-time requires comprehensive system and network monitoring, furthermore the ability to aggregate alarms and other information from disparate systems is necessary to correlate events and identify an incident.

Tactical (0-2 years)	**Strategic (2-5 years)**
NIE HP OpenView NNM 7.5 Remedy 7.0.1	IDS Microsoft Office Manager/NetIQ AppManager
Retirement (to be eliminated)	**Containment (no new development)**
	Big Brother BMC Patrol
Baseline (today)	**Emerging (to be tracked)**
Tivoli Storage Manager Dell OpenManage 3.70 CiscoWorks LMS 2.5 NIE (enVision v3.3.4 Build: 0077) Operating System Logging TMON for MVS 3.1 TMON for CICS 2.2 TMON for DB2 3.3 TMON for IMS 2.0 TMON for MQ Series 2.0	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
19	**File Transfer**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Integration	Data Integration	Data Exchange

Description
File Transfer Middleware is a class of communication middleware specifically focusing on the transfer of files from application to application. The transfer may be secure, insecure or managed.

Tactical (0-2 years)	Strategic (2-5 years)
DFS	
Retirement (to be eliminated)	**Containment (no new development)**
	FTP
Baseline (today)	**Emerging (to be tracked)**
SFTP/WS-FTP SAMBA NFS SMB	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
20	**Gateways**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Integration	Middleware	Message Oriented Transaction Oriented Object Request Oriented

Description

Gateways
There are two types of gateways:

1. Database gateways enable access to heterogeneous Database Management Systems (DBMS), usually through a common Structured Query Language (SQL) interface.

2. Communications middleware gateways connect Message-Oriented Middleware (MOM) products on the market.

Database gateways enable connectivity to heterogeneous DBMS engines, sometimes including non-relational databases, using a common Application Programming Interface (API), usually SQL, and protocol.

Integrated Adapters
Adapters are some combination of design tools and runtime software that act as glue to link applications, which are considered "sources" or "targets" (or both), to other applications or other integration middleware.

When interfacing with a source or target application, an adapter generally deals with a group of "touchpoints," that is, one or more entry/exit points, collectively called an "interface."

Adapters can be deceptively complex, with "thick" adapters performing a variety of functions that include recognizing events, collecting and transforming data, and exchanging data with platform, integration suite or other middleware. On the other hand, "thin" adapters may only "wrap" a native application interface, exposing another, more standard interface for application access. Adapters can also handle exception conditions, and can often dynamically (or with minor reconfiguration changes) accommodate new revisions of source or target applications.

Two common types of adapters are:

- *Technical Adapters* - Technical adapters may connect into DBMSs, communication middleware or other software environments. By definition, technical adapters are not inherently configured to be business process-aware.
- *Application Adapters* - Application adapters interface to packaged application modules or vertical-industry protocols (like HL7 or HIPAA). By definition, application adapters are inherently configured to interact with a source or target interface and read or write specific business documents or messages. Many application adapters include technical adapters within them. For example, an application adapter that is used to import or export purchase orders from a procurement application can leverage a technical adapter, which accesses the application at the database or low-level API level. While the technical adapter could be licensed and used by itself, the value of the application adapter is that it eliminates the need for complex logic that is often necessary to navigate what are often complex database or low-level interfaces.

Adapters are generally bundled with integration middleware products such as Enterprise Service Buses (ESBs), integration suites, or portal servers; or offered as a stand-alone product such as an adapter suite. Ideally, every adapter, like most application integration tools, should be noninvasive, such that it can interact with the source or target without requiring any customization in the source or target. Such independence helps insulate the adapter from its source or target's upgrades — for example, for new versions of software

Tactical (0-2 years)	Strategic (2-5 years)
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
21	**Identification and Authentication**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	Network Services	Directory Service
Security	Identity Control	Authentication

Description

Authenticated identities are the basis for many other information security services. Therefore, DPSCS needs to:

- Verify user identity as the basis for access control to DPSCS resource
- Control individual user access to the resources and services provided by those systems
- Create an audit trail of individual user access or attempted access to those systems, resources and services.

Authentication services are crucial to access control and auditing services. If users' identities are not properly authenticated, DPSCS has no assurance that access to resources and services are properly controlled. No matter how well managed DPSCS's access control services; everything hinges on the true identity of the user. In most situations, User ID and password combinations will provide an appropriate level of security if the User ID and password conform to DPSCS policy. However, DPSCS will implement stronger authentication for Enterprise users with high system privileges - that is, system, network and security administrators.

Tactical (0-2 years)	**Strategic (2-5 years)**
Active Directory (Windows 2003 Forest Functional Level & Windows 2003 Native Domain Functional Level)	
Retirement (to be eliminated)	**Containment (no new development)**
TACACS + - 6 months RADIUS - 6 months	
Baseline (today)	**Emerging (to be tracked)**
Checkpoint VPN (Core: NGX 60 HFA04, Edge firmware: 7.0.25) MS Active Directory (Kerberos) (Windows 2000 Forest Functional Level & Windows 2000 Native Domain Functional Level) CA Top Secret 5.3 SQL Authentication Local System Authentication RSA ACE Server 5.2 TACACS + RADIUS Rocket LDAP Bridge 2.0 SSH SSL User ID/Password Cisco ACS	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
22	**Instant Messaging**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Desktop Productivity	Electronic Messaging Collaboration

Description
The Instant Messaging (IM) Client is the user's desktop-resident software that enables users to send short, text-based messages or files to other users. IM also provides presence management to show who is online and any optional status messages posted by users. These applications allow a user to start a chat session, record the chat interchange, and invite participants to a chat room.
Note that this TAS applies to standalone IM services and that this function is often available in other applications, such as Desktop Web Conferencing and Shared Virtual Workspace.

The Instant Messaging (IM) Server is the application software that enables users to send short, text-based messages or files to other users. The server software receives presence management status from the client software and shows other users who are online and any optional status messages posted by users. These applications allow a user to start a chat session, record the chat interchange, and invite participants to a chat room.
Note that this TAS applies to standalone IM services and that this function is often available in other applications, such as Desktop Web Conferencing and Shared Virtual Workspace.

Tactical **(0-2 years)**	**Strategic** **(2-5 years)**
Retirement **(to be eliminated)**	**Containment** **(no new development)**
Baseline **(today)**	**Emerging** **(to be tracked)**
Jabber (IM Server) Exodus (IM Client)	Microsoft Live Communication Server

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
23	**Integration Broker Suite**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Integration	Data Integration	Data Exchange Data Format Data Transformation

Description
An integration broker is a third-party intermediary that facilitates interactions among application systems. By definition, the broker itself provides two primary value-added application-layer functions:

- *Transformation* - translates message or file contents, including both syntactic "conversion" and some degree of (greater or lesser) semantic "transformation."
- *Routing (flow control)* - some form of smart addressing, such as content-based routing and/or publish-and-subscribe. Note that intelligent routing is stateless.

To enable these services, a broker has some form of repository that holds metadata descriptions of the input and output message formats (i.e., a message dictionary), and the transformation and routing rules. It will also have some administration and monitoring facilities to manage the broker configuration, and may also offer application-specific or technical adapters, along with some related development tools, gateways and templates for connecting to packaged applications. An integration broker may optionally also support a message warehouse (a mechanism to store and retrieve copies of messages).

Tactical (0-2 years)	Strategic (2-5 years)
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
24	**Integrity**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Enterprise Management	Operations Management	Configuration Management Change Management
Security	Security Management	Virus Protection Spyware Removal

Description
Anti-Virus. An effective anti-virus architecture uses a multi-tier (that is, desktop, server, and gateway) approach and is not necessarily reliant on a single vendor solution. The gateway tier can be implemented at the firewall, the SMTP gateway, the SMTP relay, or a combination of all three. Using a combination of techniques at the gateway level is prudent given the frequency and impact of malicious code attacks. DPSCS currently implements a multi-tier anti-virus architecture.

Configuration Management. Configuration management is the basis for all other management capabilities and is a critical aspect of maintaining confidentiality, integrity, and availability. Change management and software control and distribution must be properly integrated with a comprehensive configuration management system.

File Integrity Checking. File integrity checking is used to detect and correct unauthorized changes to a file or database.

Tactical **(0-2 years)**	**Strategic** **(2-5 years)**
Active Directory Group Policy (Windows 2003 Forest Functional Level & Windows 2003 Native Domain Functional Level)	
Retirement **(to be eliminated)**	**Containment** **(no new development)**
WSUS Version 2 – 6 months	
Baseline **(today)**	**Emerging** **(to be tracked)**
Symantec Enterprise Antivirus Panda Exchange Secure Antivirus WSUS Version 2 SMS 2003 ScriptLogic Desktop Authority 7.5 Active Directory Group Policy (Windows 2000 Forest Functional Level & Windows 2000 Native Domain Functional Level) IronPort (Hardware version: C350 Software: 5.0.0-231)	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
25	**Intrusion Detection**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Security	Security Management	Assessment Host Intrusion Prevention Network Intrusion Prevention

Description

Vulnerability Analysis. Internet-based attack tools are becoming increasingly sophisticated and increasingly easy to use. DPSCS's network could contain vulnerabilities that attackers can exploit to gain access, even when DPSCS has secured the network perimeter with firewalls and intrusion detection systems. In order to proactively find and plug such holes DPSCS will require the use of both vulnerability assessment products and vulnerability assessment services.

System Monitoring and Logging. Identifying and reacting to security incidents in real-time requires comprehensive system and network monitoring, Furthermore the ability to aggregate alarms and other information from disparate systems is necessary to correlate events and identify an incident.

Tactical (0-2 years)	Strategic (2-5 years)
NIE NFR Intrusion Detection	Host-Based IDP/IPS
Retirement (to be eliminated)	**Containment (no new development)**
Snort IDS 2.4.5	
Baseline (today)	**Emerging (to be tracked)**
Operating System Logging NIE (enVision v3.3.4 Build: 0077) Snort IDS 2.4.5 IronPort (Hardware version: C350 Software: 5.0.0-231)	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
26	**LAN Cabling**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	LAN/MAN	*<MTAF Needs Physical Layer Technology Area>*

Description

The cabling standards document referenced in the LAN Cabling TAS in the following table should be used for specific implementation guidelines.

Currently DPSCS will continue to deploy Category 5e cabling for new installations until the need for the additional bandwidth at the LAN level is necessary.

- Category 6 solutions typically are priced at a 15–25 percent premium (including materials and labor) above Category 5e. When comparing the costs of cabling solutions, it is important to consider both materials and labor.
- Category 6 cabling delivers a usable bandwidth twice that of Category 5e. The Category 6 standard specifies a higher-quality cable that will more reliably support gigabit speeds and should be the cable of choice for all new DPSCS network installations.
- Category 6 also provides additional tolerance for some common cabling problems, such as external noise or sloppy installations. Thus, a Category 6 installation will result in fewer instances of labor intensive cable troubleshooting.

Compared to other network resources, cable and wiring have long life spans, typically lasting seven to 12 years, and sometimes as long as 15 years. Therefore, at least two generations of network technologies are likely to be deployed over whatever cabling system DPSCS chooses to deploy today.

Poor cabling decisions are costly and potentially disruptive. Correcting cabling mistakes can cost anywhere from 140 percent to 250 percent of the original cost if it needs replacing once it is already in the wall or ceiling.

DPSCS should focus its backbone on multiple 1Gbps-over-fiber links, leading to 10Gigabit-over-fiber as traffic increases and prices decline. Alternatively, DPSCS can deploy copper where there is insufficient fiber to run multiple 1,000Mbps links.

Tactical (0-2 years)	**Strategic (2-5 years)**
CAT6	Fiber Cabling (Multi mode, Single mode)
Retirement (to be eliminated)	**Containment (no new development)**
CAT5	
Baseline (today)	**Emerging (to be tracked)**
CAT5 CAT5E Fiber Cabling (Multi mode, Single mode)	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
27	**OLTP Database Server**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Database Management	Database Data Mart Data Utility

Description

The Online Transaction Processing (OLTP) database market is defined by products that are suitable for a broad range of enterprise-level real time applications, including purchased business applications such as enterprise resource planning, customer relationship management, and customized transactional systems.

Tactical (0-2 years)	Strategic (2-5 years)
IBM DB2 7.1 IBM IMS 8.1	DB2 8.1
Retirement (to be eliminated)	**Containment (no new development)**
	Microsoft Access 2000, 2003 Centura /Gupta SQL Base 8.5 Microsoft SQL Server 2000
Baseline (today)	**Emerging (to be tracked)**
IBM DB2 6.1 IBM IMS 6.1 Microsoft SQL Server 2000 and 2005 Oracle 9.2.06/ 10.1 IBM VSAM Centura /Gupta SQL Base 8.5	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
28	**Performance Management**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Enterprise Management	Capacity/Performance	Load Balancing Capacity Planning

Description

Performance Management is the trending of end-to-end response time and performance parameters from network, system and application components to predict short-term future performance degradation. This discipline assists in quicker problem diagnosis, thus reducing downtime, and can even provide advance warning of imminent problems so that they can be prevented proactively.

Tactical (0-2 years)	Strategic (2-5 years)
HP Openview NNM 7.5 Message stats for Exchange 4.1	
Retirement (to be eliminated)	**Containment (no new development)**
	BMC Patrol
Baseline (today)	**Emerging (to be tracked)**
CiscoWorks LMS 2.5 MS Perfmon NIE (enVision v3.3.4 Build: 0077) Dell OpenManage 3.70 SMS 2003 Operating Systems Logs Quest Spotlight for Exchange version 4 TMON for MVS 3.1 TMON for CICS 2.2 TMON for DB2 3.3 TMON for IMS 2.0 TMON for MQ Series 2.0 UNICOM AUTOMON 4.2.0	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
29	**Remote Access Technology**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	Network Services	Remote Access

Description

Remote access provides the ability to connect to the network from a distant location. This requires a computer, a modem and remote access software to allow the computer to dial into the network over a telephone line, cable or satellite service, and connect. Remote access via a virtual private network (VPN) creates encrypted tunnels over an existing Internet connection between remote users and the network data center.

Remote access at DPSCS is not vendor-managed and is centralized. The deployment of multiple remote access infrastructures is unnecessary and inefficient.

Security of remote access services is always a concern, as the public network infrastructure is used to deliver these services to DPSCS users.

This technical solution also allows for a corporate-wide ISP contract that can be offered as an alternative access method to users who generate the highest access charges. Such an agreement could provide VPN over local, nationwide and international dial-up access on a more cost-effective basis.

Tactical (0-2 years)	Strategic (2-5 years)
Microsoft Office / 2007 Exchange	
Retirement (to be eliminated)	**Containment (no new development)**
TACACS + - 6 months RADIUS - 6 months	
Baseline (today)	**Emerging (to be tracked)**
Checkpoint VPN (Core: NGX 60 HFA04, Edge firmware: 7.0.25) Microsoft Outlook Web Access (Exchange 2003) RSA ACE Server 5.2 TACACS + RADIUS RADIUS Database Cisco ACS	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
30	**Search Engines**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Delivery Server	Portal Server

Description

A search engine includes a robot or crawler that goes to every page or representative pages on a Website, or the whole Web, and creates an index. It also includes a program that receives search requests, compares an individual request to the entries in the index, and returns results to the end users.

This TAS addresses search capabilities for Web pages only. However, several vendors and technologies that can be used enterprise-wide (i.e., search information systems within an organization) will be tracked (in Emerging) moving forward.

Tactical (0-2 years)	Strategic (2-5 years)
Google – like search engines	
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
MS Indexing Service (Windows 2000, 2003) MS Search Engine V1.0	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
31	**Shared Virtual Workspace & Workflow**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Desktop Productivity	Collaboration

Description

Shared virtual workspaces are team-oriented collaboration tools that provide services for sharing files and supporting asynchronous and real-time collaboration activities and commentary. These applications include support for content creation, approval, and sharing; discussion boards; and offline and/or real-time interaction. Some of these applications also enable presence management, instant messaging, task management, charting and surveys.

Workflow tools allow the design, support, and implementation of specific work processes. These tools typically augment workflow with collaborative functionality, including document management, instant messaging, chat, e-mail, white boarding and other tools that facilitate employee coordination and collaboration.

These tools are common within administrative environments that require a high volume of collaboration across the organization.

As with the document management marketplace, workflow tools are moving toward the same integrated single application offering that might be found in a smart enterprise suite or a knowledge management application.

Tactical (0-2 years)	Strategic (2-5 years)
	Microsoft SharePoint Services/ EMC Documentum
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
Moin Moin Wiki 1.5 MS Exchange Public Folders (Exchange 2003)	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
32	**Staff Digital Certificate**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Security	Identity Control	Digital Certificate Electronic Signature

Description

A *Staff Digital Certificate* is a digital certificate that is issued to an individual staff member of DPSCS. A staff member is defined as anyone who possesses a DPSCS issued ID badge (e.g., employee, contractor, MD law enforcement/correctional officer, etc.). The following digital certificates are outside the scope of this standard:

- Digital certificates issued to individuals outside of DPSCS,
- Digital certificates issued to other types of entities that are not staff members, including but not limited to web services and other devices), and
- Special purpose certificates (for example, those used to support the Microsoft encrypted file system).

It is envisioned that the Staff Digital Certificate TAS will establish the DPSCS Public Key Infrastructure (PKI) as the single tactical and strategic source of staff digital certificates at DPSCS. This standard will be based on analysis of existing technologies in place at DPSCS coupled with MD and Federal Public Key Infrastructure (PKI) policy requirements. The DPSCS PKI should interoperate with other MD Agencies within a single MD-wide PKI trust domain that is cross-certified (i.e., interoperable) with the Federal Bridge Certification Authority (FBCA).

At this point, neither the state of MD nor DPSCS has any Enterprise-wide PKI solution that meets these requirements.

Tactical (0-2 years)	Strategic (2-5 years)
PKI	
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
33	**Vulnerability Tool**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Security	Security Management	Assessment

Description

Vulnerability Analysis. Internet-based attack tools are becoming increasingly sophisticated and increasingly easy to use. DPSCS's network could contain vulnerabilities that attackers can exploit to gain access, even when DPSCS has secured the network perimeter with firewalls and intrusion detection systems. In order to proactively find and plug such holes DPSCS will require the use of both vulnerability assessment products and vulnerability assessment services.

System Monitoring and Logging. Identifying and reacting to security incidents in real-time requires comprehensive system and network monitoring, Furthermore the ability

Tactical (0-2 years)	**Strategic (2-5 years)**
NFR	Third Party vulnerability assessment tool
Retirement (to be eliminated)	**Containment (no new development)**
WSUS Version 2 – 6 months	
Baseline (today)	**Emerging (to be tracked)**
Port Scanner NMAP MS Baseline Security Analyzer 2.0 WSUS Version 2 Core Securities Impact Websense	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
35	**Web Browsers**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
User Access	Access Software	Browser

Description

Web browsers are programs that “read” hypertext and display it as formatted text and images. Browsers allow users to view the contents of a site and navigate from one site to another.

Tactical (0-2 years)	**Strategic (2-5 years)**
Internet Explorer 7	
Retirement (to be eliminated)	**Containment (no new development)**
Internet Explorer 5 – 8 months	Internet Explorer 5
Baseline (today)	**Emerging (to be tracked)**
Internet Explorer 6	Mozilla-based open-source browsers

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
36	**Web Content Management**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Enterprise Management	Operations Management	Content Management

Description

DPSCS has defined web content management as a technology that automates the content creation, approval, and publication process of any digital items (e.g. video, audio, text, graphic, links to physical resources, etc.), thereby providing internal and external web accessibility, management, and search functionality based on user roles and access rights. Web content management systems are instrumental in publishing and editing inward and outward web sites. The web content management marketplace has grown stagnant and several vendors have moved out of this marketplace to focus on smart enterprise suite solutions that combine multiple collaboration capabilities into a single application. Although the market is saturated with vendors, a few vendors have established a significant presence in this marketplace and provide scalability as needed to support the users' requirements.

Tactical (0-2 years)	**Strategic (2-5 years)**
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
37	**Web Server**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Delivery Server	Web Server

Description

Web servers are software that serve as engines which run websites. Through a Web listener, they accept HTTP (non-encrypted) and HTTPS (encrypted) connections from Web browsers. The Web server may return HTML based Web pages and other files directly to the browser, or may invoke additional software that performs processes such as database interaction and generates the returned HTML or files.

Tactical (0-2 years)	**Strategic (2-5 years)**
WebSphere 7.x Microsoft Internet Information Server	Microsoft Internet Information Server
Retirement (to be eliminated)	**Containment (no new development)**
	Microsoft Internet Information Server 5
Baseline (today)	**Emerging (to be tracked)**
Microsoft Internet Information Server 6 Apache IBM Websphere 6.0.2.5	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
38	**Web Services**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Integration	Service Integration	Web Service

Description

Web services are not really a technology; they represent software components and a common set of standards supported by multiple, different technologies and vendors. Web services are Web-based services that use any one or more of three related XML-based standards including:

- SOAP - Simple Object Access Protocol, request-reply protocol for inter-program communication.
- WSDL - Web Services Description Language, an interface-definition syntax.
- UDDI - Universal Description, Discovery and Integration, defines how a directory is used to register Web services.

Web services can operate over Internet protocols. These include TCP/IP, the standard Internet transport; secure sockets; File Transfer Protocol (FTP) for uploading and downloading files to and from the Internet; Hypertext Transmission Protocol (HTTP) and secure HTTP (S-HTTP) for sending information over the Web; and Simple Mail Transfer Protocol (SMTP) for e-mail messaging; and even message-oriented middleware (MOM) and Java Message Service (JMS). The second fundamental technology is Extensible Markup Language (XML), which is the language used to create the messages, files, metadata and documents that define and describe Web services. In addition to HTTP, Web services make use of one or more of these technologies:

- SOAP lets one application invoke a remote procedure call (RPC) on another application, or pass structured data to a remote location using XML messages and the Web.
- WSDL is a formal XML vocabulary for describing Web services, their interfaces and basic implementation information for use in Web services registries and repositories.
- UDDI is a platform-neutral registry for publishing, querying, finding and invoking Web services via metadata and interfaces.

Taken together, SOAP, WSDL and UDDI form the Web services technology canon that fits atop the XML and Internet infrastructure. Here are some of the many sources for Web services:

- Applications written in Java J2EE
- Applications written in Microsoft.NET (all Common Language Runtime1 languages)
- Applications developed with ColdFusion MX
- “Wrapped” service programs from legacy applications
- Integration Broker Suite (IBS)
- Commercial off-the-shelf applications
- Commercial service providers (Internet)

The beauty of Web services today is in their simplicity. Eventually, however, complexity will creep in. Vendors (and enterprises) are developing additional layers to the existing Web services stack to address perceived (and real) issues, such as security, transaction management, user interface development, collaborative and peer-to-peer environments, business-to-business (B2B) interactions and more.

The emerging stack comes in multiple flavors, depending on the vendor, industry association or standards organization that is authoring the additions. There will be recurring attempts to build an entire stack of Web services standards that might satisfy every requirement that an enterprise might foresee, and without exception, these attempts will fail due to the vastness of their scope. Electronic business XML (ebXML) might be one such example.

More importantly, Web services standards need to fit within a larger framework that can support comprehensive enterprise requirements.

Tactical (0-2 years)	Strategic (2-5 years)
SOAP 1.1 WSDL 1.1 WS- Security and related standards XML 1.0 XML Schema Definition (XSD) http://www.w3org/2001/XMLSchema	
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
SOAP 1.1 XML 1.0 WSDL 1.1 XSD http://www.w3org/2001/XMLSchema	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
39	**Wireless LAN**	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Network	Wireless	Wireless Switching Wireless Routing Wireless Transport

Description
The role of a wireless LAN is to extend network coverage to allow for in-building or, in certain environments where core drilling is cost-prohibitive, between building communication for mobile users; wireless LAN (WLAN) equipment can also be used to create ad hoc networks for temporary situations such as conference registrations.

WLANs use electromagnetic waves to transmit data without physical connection to the access points (APs). APs act as a bridge between the LAN and wireless clients (also referred to as end users or wireless adapters). APs can support a small group of users in a given range; the theoretical number of clients supported by an 802.11b/g AP is 256 within a 100-foot range (the theoretical number of clients for 802.11a is 1,024). Depending on usage patterns, 20–30 users are recommended for optimal performance. For example, e mails with attachments require more bandwidth than e mails with no attachments, and VoIP or video applications will require substantially more bandwidth.

The range of access points is related to speed. As the distance between AP and wireless client increases, the speeds decrease, and vice versa. Building materials, floor plans and environmental factors also affect the range. For example, Gartner estimates indoor and outdoor ranges to be 100 ft. (30 m.) and 200 ft. (60m.), respectively, for 802.11b. Using a site survey tool is recommended to measure signal strength at various locations throughout the site to determine the number of and positioning of APs.

There are four main physical-layer standards for WLANs: 802.11, 802.11b, 802.11a and 802.11g. The 802.11 is the first standard and is only found in legacy installations. It is discussed here for reference purposes and should not be purchased. The 802.11b reached dominance in late 2003 and has 11Mbps data rates in the 2.4GHz band. The 802.11a is the follow-up standard that is capable of reaching 54Mbps rates in the 5GHz range. The newest standard, 802.11g, increases data rates to 54Mbps in the 2.4GHz band and is backwards-compatible with 802.11b. The 802.11b, 802.11a and 802.11g can all operate in the same environment without causing interference with each other.

The Wireless LAN TAS shown below applies to both access points and Network Interface Cards (NICs). DPSCS aims to reduce the number of vendors in the wireless AP and NIC environment in order to achieve better cost discounts and to simplify patch distribution and network management.

Tactical (0-2 years)	**Strategic (2-5 years)**
Retirement (to be eliminated)	**Containment (no new development)**
802.11 B – 3 months	802.11 B
Baseline (today)	**Emerging (to be tracked)**
802.11 G Bluetooth Cisco Access Points - 1100 Cisco Wireless Bridges – 340, 350	802.11 N

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
40	Storage Area Network	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure	Data Storage	Storage Area Network

Description

Tactical (0-2 years)	Strategic (2-5 years)
Retirement (to be eliminated)	**Containment (no new development)**
	McData (SPHEREON 4500)
Baseline (today)	**Emerging (to be tracked)**
EMC/Cisco 9509 EMC/Cisco 9216 Dell/EMC Clarion CX-300, CX-500, CX-700, CX-380 Brocade EMC Symmetrix DMX-1000	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
41	Application Development Tools	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure		

Description:

The Application Development Tools are software products from various vendors, which are used to assist in the coding, testing, debugging, and converting of the Department's computer application programs. Well written programs, which have been thoroughly tested, result in a stable and efficient computer system.

Tactical (0-2 years)	**Strategic (2-5 years)**
Retirement (to be eliminated)	**Containment (no new development)**
REX – 6 months	Centura/Gupta Team Developer 3.0
Baseline (today)	**Emerging (to be tracked)**
CA-Librarian 4.3 Compuware Abend Aid Suite - (MVS 9.5, CICS 4.5.0) Compuware Xpediter Suite - (TSO 7.4, CICS 7.5, Code Coverage 2.0, XChange 3.0.5) Compuware File-Aid Suite (Data Solutions 3.4, RDX 4.2, DB2 4.8, MVS 8.8.2, IMS 6.2.1) Assist/GT 4.6.5 QuickRef/MVS 6.5 Syncsort for z/OS 1.2.0.1 FOCUS 7.3 WebFOCUS 7.1.1 Prince MHTran-2 4.3.1 Websphere 7.x	

TAS NUMBER	TECHNOLOGY ARCHITECTURE	
42	Database Management, Design Utilities	
DOMAIN	**DISCIPLINE NAME**	**MTAF TECHNOLOGY AREA**
Infrastructure		

Description:

The Database Management and Design Utilities are software products, which aid the Department's Database Administrators in performing normal database management tasks such as: backup, recovery, reorganization, data conversion, loading, maintenance and monitoring. Properly tuned databases assist in making systems operate efficiently.

Tactical (0-2 years)	**Strategic (2-5 years)**
Retirement (to be eliminated)	**Containment (no new development)**
Baseline (today)	**Emerging (to be tracked)**
BMC DB2 Utilities - (Copy Plus 6.4.00, Admin. Assist. 7.3.02, Reorg 6.3.00, XBM 5.1.00) BMC IMS Utilities - (MAXM 1.5.00, Image Copy 3.4.00, Secondary Index 2.9.04, Pointer Chacker 4.4.00) DCR DataVantage 4.1.0 Oracle Management Tools (GRID) 10.1.03 SQL Enterprise Mgt	